IN THE SPECIFICATION:

Please amend the specification as follows:

At page 3, please amend the paragraph [12] as follows:

[12] 5. The obtained GSM key, Kc, is used as a secret, the basis of which an authenticator is computed. The authenticator may ~~to~~ be used as a session key in, for example, Mobile IP networking.

At pages 4 and 5, please amend paragraph [22] as follows:

[22] It is an advantage of the method that the extensive installed base of subscriber identification modules (e.g. GSM SIMs) can be readily used for authenticating each user in another communication system over a local wireless link. This enables a user to authenticate himself by using his/her own subscriber identity module without separately installing it into a terminal being used for accessing that communication system. Preferably, the first secret is a signed response (for example, SRES in GSM) produced at the authenticating block. Preferably, the second secret is a signed response produced by the subscriber identity module. Preferably, the subscriber's secret is a secret known only by the subscriber identity module and the authentication block (for example, Ki in GSM).The term separate refers to the fact that the communication system is or can be operated by a different vendor than the mobile telecommunications network. Typically, the communication system ~~uses~~uses a different access point or access points for connecting with the client, whereas the mobile telecommunications network has base transceiver stations for connecting with its subscribers.

At page 5, please amend paragraph [25] as follows:

[25] Preferably, the local wireless link is selected from the group consisting of: a Low-Power Radio-Frequency (LPRF) link, such as a Bluetooth link, an optical link,

such as an infrared link, and an acoustic link such as an ultrasound link. Typically, the range of the local wireless link ~~up~~is up to about 10 metres, which may vary according to sensitivity of antennas, positioning of devices in nulls, and other environmental factors. The accessing of the subscriber identity module over the local wireless link allows greatly enhanced flexibility by bringing subscriber identity module based authentication to devices that lack a subscriber identity module reader. For example, laptop computers commonly have an Infrared Data Association (IRDA) port which supports a local wireless link. In addition local wireless connectivity is expected soon in a number of different Bluetooth enabled mobile telephones and laptop PC adapters.

At page 7, please amend paragraph [35] as follows:

[35] According to a second aspect of the invention there is provided a method of ~~[SL1]~~authenticating a client to a communications system using a subscriber identity module of a mobile telecommunications network, wherein the communications system is separate from the mobile telecommunications network, the method comprising the following steps at a device containing the subscriber identity module:

At page 9, please amend paragraph [52] as follows:

[52] According to a fourth aspect of the invention there is provided a device for ~~[SL2]~~authenticating a client to a communications system using a subscriber identity module of a mobile telecommunications network, wherein the communications system is separate from the mobile telecommunications network, the device comprising:

At page 9, please amend paragraph [59] as follows:

[59] According to a fifth aspect of the invention there is provided an ~~[SL3]~~authentication system, comprising a client to a communications system and a

device for communicating with a subscriber identity module to the communications system using a subscriber identity module of a mobile telecommunications network, wherein the communications system is separate from the mobile telecommunications network, the client comprising:

At page 12, please amend paragraph [76] as follows:

[76] computer executable program code to enable the device to ~~[SL4]~~retrieve from a subscriber identity module a subscriber identity corresponding to a subscriber of a mobile telecommunications network;

At page 13, please amend paragraph [87] as follows:

[87] The term separate refers to the fact that a first communication system is or can be operated by a different vendor, provider or carrier than a second communication system. Typically, the first communication system may use ~~differenta~~ a different access point or access points for connecting with the client, whereas the second communication system may have base transceiver stations for connecting with its subscribers. Two communication systems may also be separate in the sense that each has a separate authentication system or firewall that is centrally managed by different servers.

At page 14, please amend paragraph [91] as follows:

[91] Fig. 1 also illustrates the different communications paths used for authenticating the client 110 and correspondingly generating an authenticator for a service. Each path may be a wireless link that occurs by radio frequencies, optical frequencies or sound. Single dashed lines show the paths used for authenticating and double lines show the security associations formed during the authentication process. Additionally, a security association 190 exists between the mobile station 121 and the gateway ~~190~~150. This security association represents the ~~authorisation~~authorization that may be made between a mobile station and a mobile

telecommunications network if the mobile station is used normally, for example for making a mobile telephone call. The gateway 150 may operate as a Mobile Services Switching ~~Centre~~Center (MSC).

At page 15, please amend paragraph [94] as follows:

[94] A mobile station 120 may receive the request. The mobile station 120 may decode or decrypt the request if it contains an encrypted PIN and check 211 whether the PIN of the request correctly matches a PIN stored on the SIM. Errors may be caused if the mobile station 120 and the client 110 are not ~~synchronised~~synchronized with the same time. In which case the mobile station 120 may send an error message 212 indicating that the time stamp should be verified. The client 110 may adjust the time stamp 222 and may send a second encrypted PIN 223. The mobile station 120 may receive the second encrypted PIN and may calculate whether it is correct for the SIM 213. If yes, then the procedure may continue. Either the checking step 211 or the calculating step 213 may retrieve a subscriber identity from the subscriber identity module, providing in either step, that the PIN received at the mobile station 120 is correct for the PIN stored in the SIM. The subscriber identity may correspond to a subscriber of a mobile telecommunications network. The mobile station 120 may confirm that the PIN of the request matches an identity module PIN by way of either the checking step 211 or the calculating step 213, for example.

At page 16, please amend paragraph [96] as follows:

[96] Now that the client 110 knows the IMSI or its equivalent, client 110 may send 224 an IP SIM Key Request 1 with the IMSI to the gateway 150. The gateway 150 may forward 231 the IMSI to the HLR 161. The HLR 161 may generate a number of authentication triplets, e.g. GSM triplets, typically in amounts up to three triplets. The HLR 161 then replies 242 with a predetermined number (n) of challenges, e.g. RANDs, to the gateway 150. The gateway 150 may send 232 an IP SIM key Reply 1 with n challenges to the client 110.

At page 16, please amend paragraph [99] as follows:

[99] The client may receive the at least one first secret and GSM keys that the mobile station may send 216. The client 110 only needs to have the at least one first secret verified by the HLR 161 before the client 110 can form an authentication key for using a desired service. The client 110 sends 226 the at least one first secret to the gateway 150 in an IP SIM Key Request 2. The gateway 150 may forward 233 the at least one first secret to the HLR 161, which compares 239 the at least one first secret against at least one second secret, e.g. the secret generated at the HLR or Kc. If comparison 239 indicates they match, the SIM used must be correct. After the HLR 161 determines that the SIM is correct, the HLR 161 may reply to the gateway 150 by sending 243 the second secret, which may be GSM keys, e.g. n Kc. The gateway 150 sends 234 these GSM keys to the HA 131 via the FA 141 (see Fig. 1). The FA may then grant access to the desired service for the client when the client 110 proves its identity using 227 the at least one second secret, e.g. the secret generated at the HLR or Kc.